УДК 343.98

Д. И. Шнейдерова
преподаватель кафедры правовых дисциплин
Могилевского института МВД Республики Беларусь

РЕКЛАМА В МЕХАНИЗМЕ СОВЕРШЕНИЯ ХИЩЕНИЙ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ

Известное выражение предпринимателя Людвига Метцеля, основавшего первое российское рекламное бюро, — «реклама — двигатель торговли» — приобрело широкое распространение не только среди добросовестных представителей бизнес-индустрии, но и среди лиц, осуществляющих преступную деятельность, направленную на хищение криптовалют и денежных средств для их приобретения. Реклама — инструмент, позволяющий довести до сведения неограниченного круга лиц информацию о продукте, который источник рекламирования желает продать, привлечь внимание и/или сформировать интерес к нему с целью продвижения на рынке аналогичных товаров, работ или услуг.

Криптовалюта как объект цифровой индустрии, не имеющий материального выражения, но обладающий имущественным характером, по своей функциональности может выступать в качестве расчетной единицы, товара или инвестиции, распространение которых реализуется благодаря рекламе в сети Интернет. Следует отметить, что в сфере оборота криптовалют реклама играет ключевую роль, поскольку именно на ней базируется функция приращения спроса на криптовалюты, а соответственно, и увеличение их стоимости в фиатных денежных средствах.

Рекламу криптовалют можно разделить на два больших блока: добросовестная и недобросовестная. Криминалистический интерес для научных работников и сотрудников правоохранительных органов представляет недобросовестная реклама, используемая мошенниками, вымогателями и хакерами в качестве средства реализации преступного умысла, направленного на совершение хищений в сфере оборота криптовалют. По мнению аналитиков, благодаря рекламе в 2021 году ожидается рост количества хищений криптовалют по всему миру в 1,5–2 раза по сравнению с 2020 годом, а совокупный ущерб составит свыше 4,5 миллиардов долларов [1].

Разносторонность и многозадачность рекламы позволяют классифицировать ее в рамках криминалистического исследования хищений в сфере оборота криптовалют по различным основаниям. Так, по уголовно наказуемому виду хищения рекламу можно разделить на применяемую при совершении мошенничества, вымогательства или хищения путем использования компьютерной техники. В механизме мошенничества реклама используется для привлечения внимания интернет-пользователей к продаваемым или сдаваемым в аренду за криптовалю-

ту продуктам, к участию в акциях или беспроигрышных лотереях, к инвестированию или скупке криптовалют по заниженным ценам и т. д., однако результат во всех случаях один — потерпевшие вкладывают денежные средства или криптовалюты в предлагаемый актив, а взамен не получают желаемый продукт или выгоду.

В вымогательстве и хищении путем использования компьютерной техники реклама применяется для перенаправления пользователей на специальные сайты, предназначенные либо для скачивания программ-вирусов, либо для сбора личных данных с целью дальнейшего несанкционированного доступа к криптокошелькам, банковским картам и банкингу. В случаях с вымогательством содержание рекламы может быть не связано с криптоиндустрией, но так или иначе сулит доверчивым гражданам бесплатные призы, денежную выгоду или розыгрыш дорогостоящей вещи (мобильный телефон, автомобиль, беспроводные наушники, ноутбуки и др.). Основная задача такой рекламы — активировать скачивание устройством программы-вируса, которое чаще всего проходит в фоновом режиме и остается незамеченным бытовым пользователем, или перенаправить на сайт, открытие которого автоматически начнет загрузку и установку. Принцип работы вируса может быть построен по нескольким направлениям: либо блокирует все файлы на устройстве, разблокировка которых станет возможна только после выкупа в криптовалюте, либо позволяет вымогателю установить дистанционный доступ к файлам и выбрать те, которые он в последующем будет использовать для шантажа (файлы личного характера: фотографии, видеозаписи, переписки и т. д.), либо перенаправляет вымогателю сохраненные в памяти браузера или менеджера паролей логины и пароли от аккаунтов, криптокошельков, банкингов, реквизиты банковских карт, знанием которых и оперирует вымогатель, требуя от пользователя выкуп, иначе эти данные попадут в свободный доступ в сеть Интернет или будут использованы иным образом. При хищениях путем использования компьютерной техники реклама — главный проводник к фишинговым и фарминговым сайтам (сайты-двойники известных криптосервисов), где ничего не подозревающий пользователь оставляет свои личные данные от криптокошельков, чем умело пользуются преступники. По статистике, ежедневно создается и удаляется порядка 100 фишинговых сайтов и приложений, что делает их практически неуязвимыми для выявления и принудительного блокирования государственными контрольно-надзорными органами [1].

По субъекту, от которого исходит реклама, ее можно разделить на анонимную, с указанием криптосервиса или создателя ICO-проекта, рекламу от лица знаменитых людей. При анонимной рекламе источник неизвестен, а рекламный лозунг содержит лишь призыв к активным действиям, например, «жми сюда и получи один биткойн бесплатно», «переходи по ссылке и участвуй в розыгрыше

эфира бесплатно», «жми сюда, тут раздают криптовалюту» и другие. Реклама с указанием конкретной криптоплощадки зачастую ведет к фишинговым сайтам достаточно знаменитых и имеющих признание сервисов, либо к мошенническим ICO, которые предлагают выгодно проинвестировать в развивающиеся криптовалюты за определенный дивиденд, либо к площадкам, реализующим криптокредитование с низкими процентами и минимальным обеспечением. Отдельно следует обратить внимание на рекламу с участием знаменитых людей (артисты, ученые, политики, крупные бизнесмены, модельеры, блогеры и т. д.). Мошенники, пользуясь свойством человеческой психологии доверять известным людям, активно используют фотографии, аккаунты, голоса и даже видеоролики с участием звезд для привлечения всеобщего внимания. Подобная реклама может носить одиночный характер (например, один рекламный ролик или одно объявление с участием знаменитого человека) или быть схематичной (такой механизм свойственен для блогеров, которые в своих постах ежедневно выкладывают ролики о том, как они удачно инвестировали в криптопроект и могут научить начинающих зарабатывать большие деньги так же быстро и легко, обещая даже личное сопровождение от начала до получения прибыли).

Реклама также может быть классифицирована по предлагаемому продукту: реклама ICO-проекта, сервиса по криптокредитованию, криптобиржи, обменника или распределительного реестра, товара за криптовалюту (актуальной на протяжении 2020 года являлась продажа вакцины от COVID-19 за биткойны), лотереи, розыгрыша, акции, DeFi, стейблкоинов, криптоботов и т. д. Исходя из продукта рекламирования, можно разграничить и целевую направленность: реклама, направленная на продажу товара или криптовалют, в том числе готовых проектов; реклама, направленная на выгодный обмен криптовалют на иные криптовалюты или денежные средства; реклама, направленная на бесплатное получение криптовалют либо получение двух единиц по цене одной; реклама, направленная на участие в благотворительной акции по сбору средств в криптовалюте на лечение детей, постройку приюта для бездомных животных и другие общественно полезные цели; реклама, направленная на инвестирование в ICO или криптокредитование, в DeFi и развитие стейблкоинов (криптовалюты, обеспеченные фиатом или иными криптовалютами); реклама по предоставлению услуг облачного майнинга или скупке производственных мощностей устройств пользователей; реклама по продаже героев или их способностей в онлайн-играх и т. д.

Отдельного внимания заслуживает реклама, сулящая бесплатное получение криптовалют, и реклама, связанная с майнинговыми процессами. Акции, в рамках которых мошенники предлагают бесплатно получить некоторую сумму криптовалют за прохождение опроса, рекламу сервиса пользователем в своем аккаунте в социальных сетях, прохождение игры, оставление положительного отзыва, участие в беспроигрышной лотерее и т. д., всегда сопровождаются плат-

ной верификацией или стартовым закрепительным взносом, который может взиматься как в фиате, так и в криптовалюте. Пользователь, выполнивший необходимые действия на мошенническом сайте, блокируется и уже не имеет возможности вернуть свои средства.

Реклама услуг майнинга имеет двустороннюю направленность: пользователю предлагается либо предоставление облачного майнинга для производства криптовалют за плату, либо сервис сам скупает мощности компьютера пользователя для производства личной добычи. В первом случае криптовалюта, которая была получена посредством майнинга пользователем за счет купленной мощности продавца, просто не переходит к нему на кошелек, а остается во владении облачного сервиса, объясняющего данное событие технической ошибкой или сторонней хакерской атакой. Во втором случае плата за использование энергии просто не поступает доверчивому пользователю, а сервис скрывается или ликвидируется после вывода похищенного. К слову, хищение мощностей устройств пользователей может осуществляться в автоматическом невидимом пользователю режиме за счет вирусных программ (криптоджекинг), внедряемых в систему компьютера через все те же рекламные объявления.

По предмету преступного посягательства рекламу криптовалют можно разделить на рекламу, направленную на хищение денежных средств (например, покупка криптовалют за фиат или инвестирование в стартапы); рекламу, направленную на хищение электронных валют (чаще имеет место при денежных переводах и обмене); рекламу, направленную на хищение криптовалют (продажа товаров, обмен, инвестирование, кредитование); рекламу, направленную на получение личных данных для последующего хищения криптовалют (фишинговые сайты).

Многовариантность способа доведения мошеннических рекламных объявлений до сведения пользователей позволяет классифицировать рекламу криптовалют и по данному основанию. Так, рекламные объявления могут быть размещены на криптомедийных площадках (специально образованные СМИ, блоги, каналы), в блогах финансистов и специалистов сферы IT, в аккаунтах социальных сетей (ВКонтакте, Instagram, Twitter, Facebook), принадлежащих знаменитым публичным людям, в групповых чатах в мессенджерах (особой популярностью среди русскоязычного сегмента пользователей обладает Telegram), в подборках новостей браузеров (например, Яндекс.Дзен), на почтовых платформах, видеоканалах, появляться в качестве всплывающих окон на различных интернет-ресурсах (например, в новостных сервисах, электронных журналах, играх, онлайн-казино, магазинах, на сайтах для просмотра фильмов или прослушивания музыки). Еще один метод распространения рекламы киберпреступниками — спам-рассылка на электронную почту или сообщениями в социальных сетях,

которые в большинстве случаев хоть и блокируются соответствующими сервисами, но могут заинтересовать пользователя во время очистки спам-корзины.

При этом ключевую роль в распространении рекламных объявлений играют аренда аккаунтов публичных людей или знаменитых мировых брендов в социальных сетях и покупка у поисковых сервисов слов, формирующих запросы. К примеру, такие сервисы, как Google, YouTube и Facebook, ввели запрет на размещение рекламы криптовалют, однако предоставили возможность покупки определенного набора слов, поиск которых предоставляет подборку в первую очередь тех источников, которые заплатили за место быть первыми среди однородных (мошеннические и фишинговые сайты среди них не редкость).

При реализации преступных схем хищений криптовалют реклама может быть разделена на контактную и бесконтактную. При бесконтактной рекламе пользователь, отреагировав на объявление, не вступает в связь с преступником, а лишь выполняет предложенное ему действие, например, покупает товар за криптовалюту или делает благотворительный взнос. При контактной рекламе пользователь вступает в непосредственный диалог с мошенником, который не предполагает личной встречи, а лишь общение в рамках виртуального пространства (переписка, видеозвонки, групповые конференции, установление специальной программы удаленного доступа, где преступник координирует действия потерпевшего). В основе контактной рекламы, в свою очередь, может лежать упрощенный или усложненный сценарий. Упрощенная схема подразумевает диалог между одним преступником и пользователем (чаще одно- или двукратный), направленный на вовлечение последнего в преступный замысел и координирование его действий. Сложный сценарий включает несколько этапов обмана (первым из которых выступает реклама) и действующих лиц (может быть одно лицо, но выполняющее несколько ролей). Так, пользователь, посещая один из интернет-ресурсов, натыкается на рекламу, обещающую ему большой заработок в криптовалюте за короткий срок. Перейдя по ссылке, он попадает на рекламный ролик или коллаж с изображением звезды, которая повествует свою историю заработка благодаря трейдинговому криптоботу и предлагает повторить ее успех, оставив свои контактные данные. Через небольшой период времени пользователю на электронный ящик приходит письмо от брокерской компании, которая предлагает ему внести небольшой взнос (фиат или криптовалюта) для возможности использования уникального бота (ведь в будущем прибыль будет в сотни раз больше). Недоверие заставляет пользователя обратиться к отзывам в Интернете, где благодаря купленным мошенниками поисковым запросам он попадает на «нужные» сайты с хвалебными отзывами и без сомнения соглашается на условия брокера. Потеря средств не единственный негативный результат, к которому может привести подобный сценарий. После совершения хищения

мошенники перепродают личные данные доверчивых пользователей, которые могут быть использованы вновь для преступных целей.

Таким образом, реклама — эффективное средство для поиска и привлечения пользователей — потерпевших при реализации преступных схем, направленных на хищения в сфере оборота криптовалют. Выявление и блокировка преступных рекламных объявлений имеют не только важное предупредительное и профилактическое значение, но и криминалистическое, поскольку способствуют отысканию, фиксации и исследованию криминалистически значимой информации, необходимой для построения следовой картины по уголовным делам о хищениях в сфере криптовалют.

---

1. Колобова М. Подвижный актив: объем мошенничества с токенами может достичь $ 4,5 млрд [Электронный ресурс] // Интернет-газета «Известия». URL: https://iz.ru/1130033/mariia-kolobova/podvizhnyi-aktiv-obem-moshennichestva-s-tokenami-mozhet-dostich-45-mlrd (дата обращения: 01.04.2021). Перейти к источнику